

ADVANCED WINDOWS

Recovering from a virus attack

Even the most vigilant of PC owners can suffer from a virus attack. Simon Edwards explains what to do in the event of an infection and provides tips for tightening up your security

It's very likely that your PC will encounter a computer virus, spyware or attack over the internet at some point. If you follow our regular advice of running good anti-virus software, a firewall and keeping Windows and other applications updated, your PC is relatively safe. However, there is always a chance that you or someone else with access to your computer will click the wrong button, visit the wrong website or let down your defences just long enough for the computer to become infected.

When that happens, you can dig out this article and use it to recover from the mess that your PC has got into. Even if your security is watertight, knowing how to recover an infected system can come in handy when friends and family get themselves in a state. We'll even show you how to disinfect a mobile phone.

SEEING THE SIGNS

It's easy to blame a virus the minute something goes wrong with your computer. When Windows slows up, blue error screens appear and files become corrupt, many people ignore the most likely reasons, such as failing hard disks, and jump to more exciting conclusions. The following symptoms will help you diagnose an infection more accurately.

If you start seeing pop-up adverts even when you're not using the web, combined with very slow performance, you can be fairly sure that you have a spyware infection. If your hard disks suddenly appear to be full, even if you can't see the files, you may have a virus infection. If your friends and colleagues complain that you've been sending infected emails, it's possible that your system has been infected.

This is not a sure thing, though. It used to be that email viruses simply sent themselves to contacts in a victim's address book. Modern variants often falsely claim to originate from one of these addresses, which makes it difficult to determine who in your circle of contacts has been infected.

Programs opening on their own, sounds playing and activity on CD, DVD and USB flash drives all indicate

that your system is being remotely controlled by some backdoor software, which may have arrived as a virus, Trojan or spyware.

You should also look out for strange error messages and note them down. This is particularly important for error messages in foreign languages, which indicate that a virus or backdoor has installed itself. We can use the text in the error message to identify the virus. Knowing which virus is on the system makes removing it much easier.

IDENTIFYING THE PROBLEM

If you know what has infected your PC, that's half the battle won. The easiest way to find out is to run an online virus scanner. We recommend online scanners because they let you check your computer with a different anti-virus program than the one you have installed. If your computer is truly infected, your regular anti-virus software will have missed this particular virus and you'll need a second opinion. There are some useful scanners at www.kaspersky.co.uk/virusscanner and <http://housecall.trendmicro.com>.

While online scanners may detect the virus, not all will remove it. They should at least provide enough information to identify it, though. If you are lucky, it will also delete the infection or provide a link to a free tool designed to remove that specific type of virus.

If your PC is unable to connect to the internet, you may have to use another computer to research the symptoms and download the free removal tools. If you have nothing more than a note of a strange error message, use an online virus database such as the one at www.symantec.com/security_response. Search for the error message and you should discover the name of the virus that caused it.

REMOVING THE VIRUS

Now you know the name of the virus that has infected your computer, you can attempt to remove it. You may be able to do this manually, without the aid of a removal tool. If you are feeling brave, read the

INTRODUCTION

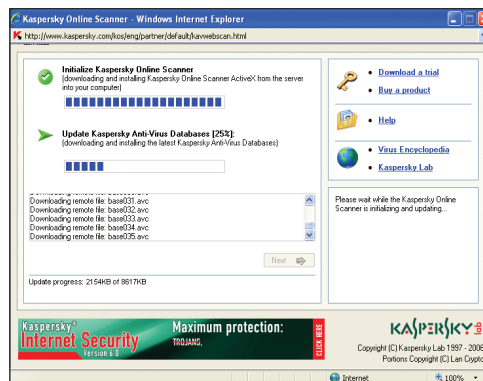
Personal computers have revolutionised our lives, but there is a dark side to the convenience and power that they provide. Computer viruses exist that can destroy your files, take over your computer and send masses of junk email.

No matter how careful you are, there is always a chance that your system will become infected with a bad program. Here we show you how to get back up and running after a virus attack, and how to stop it happening again.

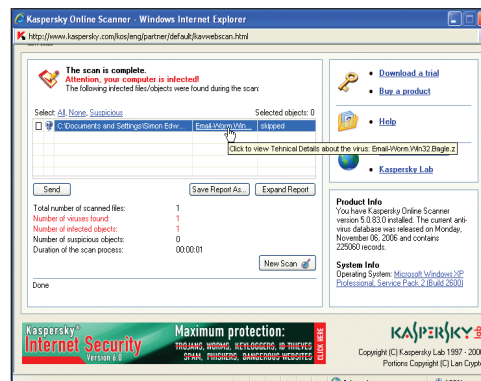
Simon Edwards
Technical Editor



windows@computershopper.co.uk



▲ Kaspersky has a very useful online scanner at www.kaspersky.co.uk/virusscanner



▲ The online scanner may not be able to remove the virus but it provides information needed to identify it

technical documents you've found on Symantec's or Kaspersky's websites. Note where the virus files will be installed and what Registry keys are used to run it and get to work with RegEdit.

For most of us, using a free removal tool is a better idea. Symantec has a long list of these at <http://tinyurl.com/eqzyq>, and there are some others at www.kaspersky.co.uk/removaltools. McAfee takes a slightly different approach and provides a single downloadable tool called Stinger, which is able to remove a number of prevalent viruses. It is available from <http://vil.nai.com/vil/stinger>.

Depending on the software you use, you may be given the option of deleting or cleaning a virus. Often a virus will be a file or collection of files on your hard disk. In this case, deleting the virus is the only viable option. However, sometimes a virus will infect a legitimate executable file, such as Explorer.exe or Word.exe. In such cases, anti-virus software may offer to



◀ Symantec has a long list of free removal tools available at its website

excise the bad code from the good. But should you allow this?

REINSTALLATION PROCEDURE

Even anti-virus programmers acknowledge that removing virus code from inside a legitimate program is hard. There is always a risk that bits of virus code will be left behind, in which case the legitimate program may become unstable or simply not work any more.

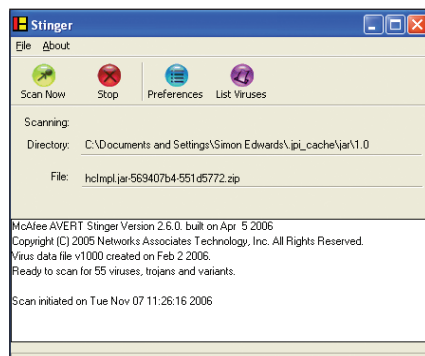
If you have the installation media of the affected program, reinstalling it is the easiest way to get a working system running as quickly as possible. Restoring files from a backup will work, too, although you should do this only if you are sure you made the backup before the system was infected. Otherwise, you may end up with another infection, which increases the chance of more damage being done.

It is always worth trying to work out when your system became infected, because then you can attempt to clean your backups or simply delete them. The name of the virus you have been dealing with can help, as anti-virus websites usually list the dates when each variant first appeared. This is a useful guide, if nothing else.

If your system doesn't have much software installed, if you don't need to use the PC urgently and if you have time, the sure-fire way to get a clean PC is to reinstall everything from the original CDs and DVDs. This is the most dramatic option and should be unnecessary in most cases.

IDENTIFYING OTHER THREATS

We've talked mainly about viruses so far, but there are other threats that you are likely to come across. Spyware is one example, and this type of bad software is becoming more



▲ McAfee's Stinger is a single downloadable tool that can remove a number of viruses

HOW TO... Use System Restore

Windows System Restore protects certain files so that they can be restored in the event of a disaster. For example, if you edit the Registry you might make a mistake that causes Windows to run incorrectly. System Restore makes undoing your work easy. However, as well as protecting legitimate files it also isolates infected ones.

This means that anti-virus software may detect a virus in the System Restore storage area but it won't be able to delete it. This is annoying, resulting in virus alerts every time you run an anti-virus scan. Even worse, once

you have wiped the virus from the main part of the computer there is a chance that it could re-infect the system later.

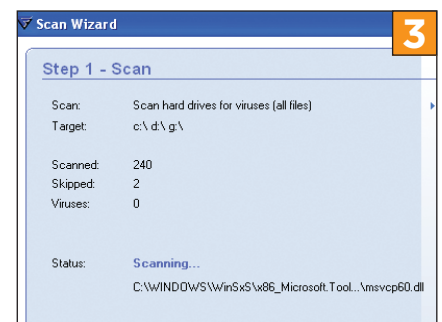
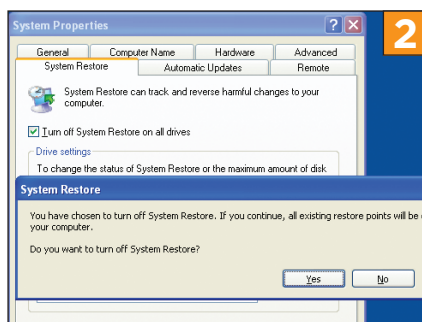
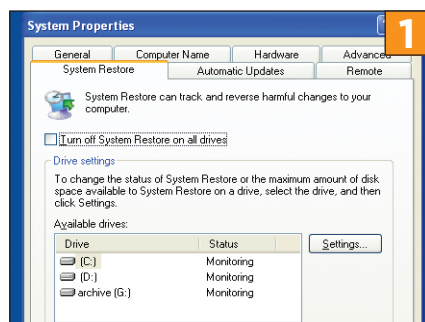
If you restore files from an earlier time, when the computer was infected, the virus files will be reintroduced and you'll have to clean it all over again. Always turn off System Restore before cleaning a virus. This might sound counter-intuitive, but failing to do so just creates trouble for later.

1 Open the Control Panel and double-click the System icon. Click the System

Restore Tab to see if System Restore is enabled and, if so, which drives are being protected.

2 If it is running, tick the 'Turn off System Restore on all drives' box. You will receive a warning that all your restore points will be lost. Unfortunately, you have to accept this.

3 Run an anti-virus scanner and ensure that it detects and removes the virus you know exists on the system. After it has finished, return to the System Restore window and untick the box in Step 1.



sophisticated, often sharing many techniques virus writers use to hide their programs.

Although you can buy specialist anti-spyware software, a good anti-virus program ought to protect you just as well. Because of this, using the techniques described here is as applicable to spyware as it is to viruses, although free removal tools and online scanners are harder to find at the moment. Try using the Kaspersky online scanner if you suspect a spyware infection. When we tested anti-spyware software in Labs, *Shopper* October 2006, our Kaspersky Anti-Virus 6 software detected every piece of spyware we encountered. The Scan version of Webroot's Spy Sweeper, which also did well in our Labs review, is included on this month's cover disc.

If you want to see what the latest spyware threats are, there's a list at <http://research.sunbelt-software.com>. This provides links to technical details such as what files the spyware places on your PC's disk and what the symptoms of the infection are. There is even a so-called Automated Malware Sandbox feature that lets you upload suspect files and see what they would do (or have done) to your computer.

Spyware comes in many shapes and sizes. We covered this subject in some depth in our spyware feature 'Spies in the Machine' (*Shopper* October 2006). Since then, some interesting developments have taken place and spyware writers are using new techniques to trick us into installing their bad programs. Spyware often comes as a Trojan; it appears to be something attractive, but contains a nasty surprise. When targeting users after free pornography, for example, spyware writers package their goods inside a video-player program. The latest trend is to distribute software that pretends to be a codec update for Windows Media Player that has been designed to allow adult movies to play.

Trojan-Downloader.Zlob.Media-Codec is one such program. It claims to be an adult codec but downloads bad software secretly on the victim's PC. This includes rogue security software such as SpywareQuake, as well as a backdoor that allows the attacker to control your PC remotely.

TACKLING PHONE VIRUSES

Viruses don't just exist on Windows PCs. The increasing number of Bluetooth-equipped phones means that virus writers have already started writing software that can jump from

one phone to another. As powerful smartphones become more popular, it's only a matter of time before this kind of threat becomes a problem.

At the moment, there are very few mobile phone viruses, although there are two notable ones. The first known mobile phone virus was Cabir, which scans for other Bluetooth-equipped phones and attempts to send an installer file to those it finds. Anyone who allows the file to install will have an infected phone that does the same thing.

The CommWarrior virus behaves in a similar way, although it also uses text messaging to spread. It attempts to contact Bluetooth phones within range and also sends SMS messages to contacts in the phone's address book. This widens its range and could prove expensive to the person signed up to the contract, if nothing else.

Turning off a phone's Bluetooth Discoverable mode prevents an infection from Cabir and not installing incoming software that you weren't expecting protects you from CommWarrior. Both of these viruses affect Symbian-based phones, but it is surely only a matter of time before Windows-based smartphones are exposed to similar threats. The virus writers are only waiting until these become more popular, because then it will be worth their while.

SAFETY LAST

So you've rescued your system from a virus infection or reinstalled from scratch and vowed never again to make the same mistakes. How can you prevent this sorry situation happening again? If you follow our standard security advice of running an up-to-date system armed with the latest anti-virus and firewall software, possibly as well as a dedicated anti-spyware utility, your chances of becoming infected with a virus or spyware are greatly reduced. However, the threat still exists.

Running a hardware firewall, as well as a software one, is a good idea. If you use ADSL with a router, you've probably already got one. Check that it is enabled. Cable users should invest in a suitable router, such as the D-Link RangeBooster N 650 Router, which we reviewed in *Labs, Shopper* November 2006. It costs £95 including VAT and will provide your network with fast wireless as well as protecting it with a decent firewall.

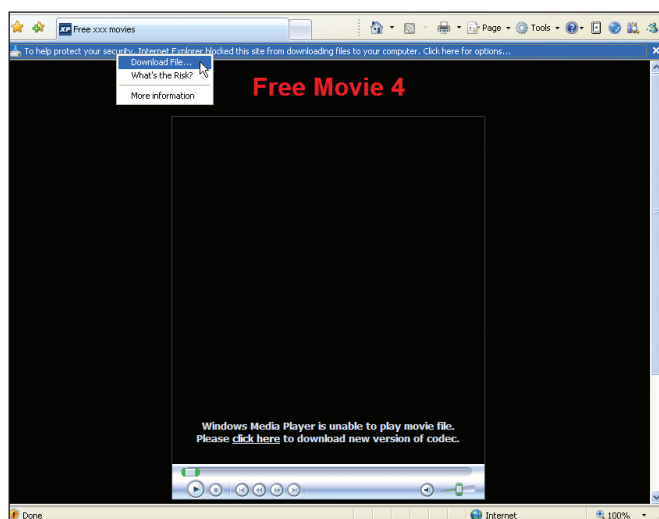


▲ The CommWarrior mobile phone virus uses text messaging to spread

If your ISP or email provider includes email anti-virus scanning, turn it on. Their systems may miss some viruses, but any obstacle you can place between yourself and the virus writers is a good thing. 'Defence in depth' should be your maxim. Some anti-virus programs come with extra protection features sometimes known as Application Control or similar. These notice when a program has changed and can prevent it accessing the internet or even running at all. However, these useful features can reduce your PC's performance and may not be turned on by default. Check these settings and turn them on where necessary.

TRUTH HURTS

Finally, be honest with yourself. If you intend to explore the more dangerous parts of the internet, where adult movies, cracked software and other dubious files lurk, be very careful and accept that you are doing something that is putting your PC's security at risk. Using a sacrificial PC, which you are happy to restore from a backup at a moment's notice, is more sensible than using your main computer to look for nude pictures of Paris Hilton. However, avoiding that whole area of the internet is by far the safest option from a PC security point of view, as well as a legal one. And Paris Hilton should be avoided at all costs, anyway. **CS**



▲ Some spyware writers distribute software that pretends to be a codec update for Windows Media Player



▲ Some anti-virus programs come with extra protection features, known as Application Control or similar, which notice when a program has changed